

Chapter 22

Network Preventive Maintenance

A network is a collection of electrically-powered pieces of equipment, connected via cables, and running programs. In order for the network to work properly, every piece of the network must work properly. *Network preventive maintenance (NPM)* is concerned with anything that can be done to prevent any component of a network from failing.

A network is not just computers; therefore, NPM is not just concerned with blowing dust out of PCs. Each component of the network (cabling, servers, workstations, peripherals, and so on) has its own special usage and maintenance concerns that must be dealt with in order to provide maximum network reliability.

While proper preventive maintenance of any sort provides the opportunity to detect and correct problems before they become failures, it cannot prevent all failures. No amount of preventive maintenance would have saved the *Titanic*. Similarly, if you are driving down the road, then suddenly close your eyes and let go of the steering wheel, you will crash no matter when you changed the oil, washed the windshield, checked the brakes, or had a tune-up. I don't believe anyone thinks that proper maintenance makes an automobile last forever. All good automobile maintenance can do is provide maximum utilization with minimum downtime for the life of the car. Just as no car drives forever, no network runs forever. All a good NPM program can do for your network is detect and prevent more problems than if NPM were not done. No NPM program can possibly detect and prevent all failures, and eventually any network will have to be replaced.

The NPM program itself does not determine the reliability of the system—the quality of the system is the most significant factor. A low-quality system requires more preventive maintenance than a high-quality system, and since preventive maintenance cannot detect and prevent all failures, a low-quality system usually has more failures than a high-quality system no matter what preventive maintenance program is in place. You never get the same reliability from a used Yugo with 150,000 miles on it that you get from a new Mercedes, no matter what kind of preventive maintenance is done to the Yugo. Therefore, the results of any NPM program depend on the quality of the network

itself. This means more than just hardware components—a network is a collection of hardware and software, all connected somehow. The quality of the software, connections, and how everything is assembled has to be taken into account when assessing the overall quality of a network. The best NPM program in the world is for naught if your cable plant is punched down with a pocketknife, your PCs are second-hand clones, you use only discount software or shareware, every time you install any software you do it differently, and your network documentation consists of a folder holding user's guides for *some* of your computers. The quality of the network is determined not only by the quality of the items you buy, but also by the quality of the effort made to install and keep track of these items.

There are three things that need to be done before you'll have a successful NPM program:

1. Do it right the first time.
2. Duplicate it the same way every time.
3. Document everything.

The following sections explain “The Three Ds” in detail.

Do It Right

This idea is so trite that it's almost useless. Even when it's stated as, “If you have enough time to make it right, you have enough time to do it right in the first place,” most people hear the idea without really understanding or believing it. I have never heard of any study that has shown it is more effective and cost-efficient to fix a problem than to have done it right the first time. It is my experience that 99% of the things I do right continue to work, while 99% of the things I do wrong eventually fail. I have found that if I do something well today, I may have time tomorrow to do what needs to be done tomorrow. But if I do that thing poorly today, I have to not only do tomorrow's work tomorrow, but also redo today's work. It doesn't take long before the day arrives that I spend all my time redoing previous work.

(This means doing it and testing it myself. I won't say that something works until I've installed and tested it. I don't care if it is “supposed to work,” “could work,” or even “has worked” in the past. I've been burned too many times—by incompatible drivers, old DLL files, different versions of the hardware, defective equipment, and just plain old lies from the manufacturers—to make a commitment based on anyone else's word. Actually, no one who has worked with PCs for very long puts much faith in “The manufacturer says it will work” or “According to the spec sheet, we should be able to do this.”)

The trick, of course, is knowing what “right” is. With all the new equipment and software that comes out, it is almost impossible to keep up with the various ways that new systems can be installed, set up, configured, and run, let alone the possible ways to make these systems interact. Add to this the fact that there is not necessarily just one way to do things right, and the mandate to “do it right” appears practically impossible.

Fortunately, there is a way to proceed even if you're not 100% sure that you're doing things exactly right—duplicate what you do.

Duplicate It

Do whatever you are doing the best way you know how, and then duplicate it whenever possible. This is one of the most powerful and least utilized tools available. Doing something the same way every time benefits you in two significant ways, even if you're not doing that thing right:

- Quicker and more thorough testing of your configuration

By doing something the same way each time, each installation is testing the same configuration. If you do it differently each time, then you have single installations testing their own configurations. For example, if you install the same piece of software the same way on 20 workstations, you end up with one configuration being tested by 20 workstations. If you install the same software differently on the 20 workstations, you have 20 configurations being tested by one workstation each—this is not as beneficial. The more testing you do, the quicker problems should show up and the sooner you should be able to make things right.

- Easier fixes and upgrades

If you find you need to fix something or upgrade it, it's far easier to figure out how to do it for one configuration than it is for multiple configurations. Fixes are inevitable because nothing is perfect, and upgrades are inevitable because technologies keep changing. Implementing a fix or upgrade on a unit is sometimes more difficult than installing something from scratch. Where you can decrease the difficulty is in subsequent implementations. If the second unit that needs a fix or upgrade is the same as the first, it's just a cookie cutter procedure. If, on the other hand, the second unit has a different configuration, it can be as hard as (or harder than) the first implementation.

By doing it as right as possible the first time, you make things work better for longer periods of time than if you implement quick-and-dirty shortcuts. Duplicating whatever you do allows you to test your configurations more quickly and thoroughly than doing custom configurations, and it makes fixes and upgrades much easier to implement. Even if you don't do it right or duplicate it, there is a tool at your disposal that will help you maintain your network and your sanity—document your work.

Document It

The partner to my “If I haven't tested it, it doesn't work” point of view is “If it isn't documented, it didn't happen.” Not having its configuration documented obviously does not stop a computer from operating. Until it is documented, though, it cannot be maintained, upgraded, or fixed.

Chapter 22—Network Preventive Maintenance

Unless you have access to a great deal of information about each and every component of a network, I submit that you cannot maintain it. If you don't know which directory an application is in, how can you upgrade it? If you don't know what the IRQ and address settings are for the NIC, how can you configure the new network driver? If you don't know which make and model of NIC the computer has, how can you know what driver to use, let alone how to configure it? If you don't know where the station jacks are and what their numbers are, how can you move or add equipment? This information has to be known in order for there to be any maintenance of the system. It can either be done on an ongoing, systematic basis, or else be done in a panic at the last minute. One way or the other, you have to write down the information before you can make any plans, purchase any equipment, or implement any fixes or changes. Having it in your head doesn't qualify.

It is important to keep in mind that documenting a system is not a one-time affair. Just like you don't balance your checkbook once and then forget it, you should not document your network once and then forget it. You keep updating your checkbook ledger because you keep making transactions and want to keep track of the current balance. In the same way, your network keeps changing and you need to keep track of its current status. Also, just as monitoring your checkbook might make you notice that you tend to always end up with the least amount of money near the end of the month, you can track your network's problem areas by writing down all relevant information and comparing today's information to previous information. Every time your network changes, write down exactly what changed. Periodically, sit down and reconcile your documentation to make sure that what you've written down agrees with what is really out there!

I don't know of a best way to document a network, or of any program that makes it a painless process. Every time I've investigated programs that have purported to do it all, I've found them lacking in some important feature, usually difficult to use, and expensive. In the meantime, I have found it works best for me to make changes on a piece of paper, since I don't always have access to a computer. But the changes have to be fed into a computer-based data file in order for the information to be analyzed and organized. Whether the data file is a spreadsheet, database, or even a word processing document depends more on how and why I am collecting the data, and how comfortable I am with the application. Since most projects and environments allow little or no time for documentation, I do the best I can with whatever time I can allocate for it.

If you do it right, duplicate it, and document it, I think you have every reason to expect a reasonably running and maintainable network. Even if you don't do it right or duplicate it, you've got a fighting chance as long as you document what you *are* doing. The more documenting you do, the more reliable and maintainable your network becomes. The less documenting you do, the less reliable and maintainable your network becomes.

In the following sections, we discuss these concepts as they pertain to the various components of a network, and examine NPM concerns for each component.

AC Power

Every piece of equipment on your LAN requires electrical power. Even the hubs and MAUs that do not plug into AC outlets get their power from something else that does plug into an AC outlet. There might not be much you can do about the power the utility company provides you, but that increases the importance of what you *can* do.

Do It Right

Until you know you have good, clean power, you always have to factor power problems into any troubleshooting situation. How can you make sure you have good, clean power? Base this information on actual tests of your power, not someone's casual assessment. Failures caused by power problems can cost you dozens of hours of troubleshooting, as well as thousands of dollars.

Duplicate It

Make sure all your wiring circuits are equivalent. Don't mix and match circuits of different load capacities, or put twice as many outlets on one leg as on another.

Document It

Make sure you have an up-to-date floor plan that includes the electrical wiring diagram. It should indicate where the circuit breaker panel and outlets are, and should clearly show which outlets are on which circuits.

Dos and Don'ts

Don't just assume that you have good power. Until it's been tested, assume you don't. Show your concern for your LAN server and associated equipment by having a special dedicated and isolated ground circuit installed just for them.

UPS System

Your UPS system is supposed to protect your critical equipment and provide enough battery-powered runtime to allow it to be shut down properly during a power failure. As such, it typically spends 99.99 percent of its time doing very little, but then suddenly needs to be doing its job exactly right to prevent a very serious problem. Proper preventive maintenance for your UPS system is essential if you want to be able to rely on it.

Do It Right

Make sure your UPS system is large enough to handle the load of all the equipment you have plugged into it. Also, while we usually think of UPSs as providing power during a power failure, they should also provide complete protection from sags, spikes, surges, EMI, and RFI—make sure that yours does.

Duplicate It

If you have more than one UPS, keep them the same. This means the installation and maintenance procedures are the same, reducing the chance for errors. It also means that you have 100-percent swappable units. If the UPS on your most important piece of

equipment fails, you can replace it instantly with the UPS from another, less-critical piece of equipment without spending a full day reconfiguring it.

Document It

Keep copies of the original invoices, and register the units for warranty purposes. Document the expected battery life and make a note on your to-do list that informs you well in advance of this date. Document all test and monitoring results, and analyze them periodically for any trends or aberrations.

Dos and Don'ts

Do line up procedures and budget dollars to replace the batteries well in advance of their expected failure date. Test the unit regularly and document the results. Don't plug any additional equipment into an existing UPS without checking the load capacity of the UPS. Dispose of used batteries safely and properly. Higher temperatures decrease a battery's life, so don't place the UPS in an unventilated and crowded cabinet.

Cable Plant

Besides electricity, the other component of the LAN that every piece of equipment shares is the cable plant. No matter how varied or large your network, everything depends upon the connecting cabling to be working at 100-percent efficiency at all times. Cabling problems are among the most aggravating and frustrating problems to deal with, but a little preventive maintenance goes a long way in preventing cabling-related problems. Since the cabling literally just lies there, once you get it right it tends to stay right.

If you only have enough budget money to test either the AC power or the cabling, get the cabling tested first. There is less that can go wrong with AC power, and almost nothing you can do about AC power problems. On the other hand, there are many things that can go wrong with your cable plant, and there fortunately are many things you can do to fix these problems. Get your cable plant tested as soon as you can, and prepare to be surprised.

Do It Right

Make sure that your cabling has the capacity for, and is designed to work properly with, the kind of network you are running. Anything less than Category 3 (Cat 3) wiring is unacceptable for today's networks. Category 5 (Cat 5) wiring is typically installed today. Also, all the wiring needs to be the same—a common problem is mixing different grades of wiring in a network. Maybe the original network was Cat 3, but some stations have been pulled using Cat 5, and the patch cords are a mixture of Cat 3 and Cat 5. Or maybe some silver-satin phone cabling was thrown in, just to make things interesting! (The silver-satin cables used for phone wires are *never* acceptable as network wiring.) According to Frank Leeds of Seitel, Leeds, and Associates, a certified cabling expert, mixing different grades of cabling creates impedance mismatches that can cause problems for your network.

The wiring itself is not the only thing that needs to be category-certified. All the connectors, punch-down blocks, patch panels, hubs, and station jacks need to have the same rating as the wiring. If you scrimp on one link in the chain, you've crippled your entire cabling system.

Of course, using all the best components won't do you any good if the wiring is not installed properly. Crossing wires, untwisting the wires too far from the connectors, or not securing connections properly can kill any cabling system. A quick survey of your wiring closets and a couple of station jacks should give you a good idea of what your whole cabling plant is like. The best thing to do, however, is to get your cable plant tested by a certified cable installation company. Each and every run of wire needs to be tested to ensure that it meets the specifications of that category level. Since this test typically includes everything from station jacks to patch panels, it eliminates the need to test each component individually and also indicates the overall quality of the installation. If the numbers aren't up to specification, you'll have to start digging in to find out if you have substandard wall plates, poor installation, or possibly even the wrong cabling.

Duplicate It

Wire all the jacks the same way. Avoid having different station jack configurations as much as possible. This is likely to confuse you, and guaranteed to confuse your users. While it is an easy fix to make, unplugging a telephone from a data jack can be avoided.

Make sure that you have specifications and part numbers for all the components of your cable plant, so that when (not if) you have to add more pulls to your plant, they can exactly match your existing pulls.

Document It

Documenting the cable plant is a classic case of "pay me now or pay me later." It is so tempting to finally get everything working, and then just walk away from it. Once it is working, it shouldn't break, so why bother documenting it? Here's why—because there is no way that your computer system and phone system will not change in the next few years. Every minute spent documenting a cable plant upon installation would have to be multiplied by ten to do the same job down the road. Besides, what better time to straighten out any problems than right after the contractor has supposedly done the job right? Trying to get a cable plant documented and fixed before any changes to it are made almost never finds a place in the time and money budgets. Consequently, future changes are usually implemented based on assumptions that bear no relationship to reality.

Once, I was involved in installing a number of servers and workstations for a client. I was assured that the wiring was already handled. When it was time to plug everything in, we found that while all the wiring and components were indeed Cat 5, all the station jacks and patch panel ports had been wired for terminal communications, not for 10BaseT Ethernet. At the last minute, then, we had to purchase and install several hundred adapters to make the system work. As if that weren't bad enough, one site had previously reconfigured their wiring so many times that none of the labels were correct anymore,

Chapter 22—Network Preventive Maintenance

and we had to find and label each run ourselves. Proper documentation of the components and station pulls would have avoided the whole problem.

Documentation should include not only a marked floor plan, but each pull should be plainly, clearly, and unambiguously marked on each station jack and its terminating end in the wiring closet. Some people even label the patch panel to hub cables, but I personally find this to be of little use, as long as you use proper wire management accessories.

Dos and Don'ts

Do assume that any cable plant—new or existing—that has not been tested and documented is out of compliance with specifications. If you have an untested plant, get it tested and documented immediately.

If you are installing a new plant, make sure that the installation contract includes a test for each pull. All the results should be provided to you. Once the contractor is done, plug in a server and carry a laptop around to each port to verify that it can connect to the server before accepting the job.

Just because the contractor can pull a wire from one corner of your building to another doesn't mean it will work. Ethernet typically is limited to 100 meters (about 300 feet) from hub to workstation. Make sure you know and stay within the limits of your particular wiring and networking specifications (see chapter 7, "Major Network Types").

Hubs/MAUs

Keep hubs and MAUs dry and clean; also, make sure that you know what all the blinking lights and switches do. If you are having a system failure that you think is caused by something in the wiring, it helps to know if the light on your hub or MAU is supposed to be flashing green or solid red to indicate normal operation.

One time, I spent almost an entire day trying to upgrade an existing gateway on a LAN. We'd installed a new gateway and shut the old one down for a week while we waited to see if the new one was going to work. When it tested okay, I upgraded the software on the old gateway and tried to reconnect it to the LAN. It just wouldn't work. I redid the installation three or four times, then I downloaded and installed patches that the vendor had said could solve the problem. Finally, in exasperation, I walked over to the MAU rack and noticed that all the ports had switches. The switch for the port this troublesome gateway was on was switched differently than the others. It turned out that the switch isolated the gateway from the token-ring network. Someone at the company had flipped it because it was their standard procedure for unused ports. I flipped the switch and everything was just fine.

Don't forget to clearly mark all units, as well as the cables interconnecting the units, with descriptive identifiers.

A rule of thumb that has solved or prevented many problems for me has been to never mix different models of hubs or MAUs, let alone different vendors. I don't care how compatible a vendor claims their unit is with your installed devices. If you can't get any more of the old units, it's time to replace everything. Life is too short to spend it trying to track down incompatibilities between different makes and models of hubs and MAUs.

Backup/Archival System

While you might get by for quite awhile without doing any preventive maintenance for your AC power, UPS, or cable plant, almost no one can survive for long without a proper preventive maintenance program for the backup system. You might still have a job after a system crash that is caused by an equipment failure, but it's probably time to dust off your resume if you have a system crash and can't restore the backups (for any reason). There are so many ways for a restore to not work, that failure to implement a comprehensive preventive maintenance program for your backup system is tantamount to career suicide.

Do It Right

Install a backup/archival system that meets your needs. I prefer a system that can back up everything, every night, unattended, but sometimes the budget isn't there for this sort of "ultimate" backup system. Whatever system and rotation schedule you have, the most important preventive maintenance you can do for your system is to understand what it does and doesn't back up, and know how to get the data back! It's amazing how many backup systems are set up and then forgotten. I've seen more than one system where an unlucky assistant was popping tapes into a tape drive as regularly as clockwork—but the software wasn't configured to back up the appropriate files, or the tape drive had stopped functioning a long time ago. Since no one knew how to restore a file, they had never tested the success of their backups, until it was too late.

One time, I set up a system to back up everything in the single volume the user had. I did a test backup and restore, documented the procedures, trained the operator, and left. Some months later, they had a crash and couldn't find all their word processing files. After much research, it turned out they had upgraded their word processor to a newer version that created a different subdirectory in the root of the volume. Their backup software was backing up only those directories that existed at the time it was installed, and all new directories were ignored.

One of the first jobs I had as a LAN analyst for a Fortune 500 company was to straighten out a problem with their backup systems: they were using name-brand hardware with name-brand software, but not getting reliable backups. I discovered that they had turned VERIFY to OFF in order to have the backup completely done before the start of business each day. I turned VERIFY to ON at seven sites, and the next morning four of the seven units reported failures. It turned out that VERIFY not only meant to verify that what was written matched what was on the disk, but actually to verify that *anything* was written. Four of the seven tape drives were defective and hadn't been writing a thing to the tapes. With VERIFY turned OFF to save time, the system was never checking to see if anything had been written to the tape at all. We fixed the drives, kept VERIFY set to ON, and adjusted the backups to only back up and verify as much as they could each night. It meant changing from a full system backup each night to a differential backup, but at least we had some idea if the backup was failing or not.

Duplicate It

Most networks don't require multiple tape backup or archival systems. If yours does, however, then by all means duplicate whatever works. Backup systems have too many complexities, quirks, and idiosyncrasies for you to wrestle with more than one type of system at the same installation.

Document It

Write down which tapes rotate in and out, and when they are to be used. Note which tapes are stored off-site. Make a list of nightly backup procedures, post-disaster restore procedures, and at least three people who are trained and tested in restoring files. Finally, document procedures for determining which files have been backed up to which tapes.

Dos and Don'ts

Don't assume that because backup software gives you no errors, everything is okay. (I ran one program from a batch file that kept automatically clearing the screen of error messages before I could read them!) The only reliable and truly meaningful test of a backup system is to restore a file or set of files. Restore at least one random file from each backup set to be sure that the backup worked. This does two things for you: it tests to make sure the backup worked, and it keeps you practiced at restoring a file or set of files in case of emergency. There's nothing as stress-inducing as having the president of the company come barging into your room, demanding to know why the files haven't been restored, as you're flipping through the manual trying to figure out how to do it. Practice makes perfect, and helps you keep your cool—not to mention your job.

Clean the heads of your tape drives as the manufacturer says to do. Most drive manufacturers provide a head-cleaning cassette and recommend a certain cleaning schedule. Write down each cleaning on the cassette's label, including the date and initials of the person who did it; leave this cassette near the tape drive so that there is no excuse for ignoring it.

Maintain a book with the backup schedule in it, providing space for initialing by the person who starts the backup and the person who tests the backup.

Workstations

Every time I think I've found a great preventive maintenance for workstations, I discover I'm breaking about as many units doing the preventive maintenance as the number of units I am possibly saving from premature failure. I thought that cleaning floppy disk drives made a lot of sense until I read an article by a drive manufacturer that stated most of the cleaning solutions being used were more destructive than just letting gunk build up. I thought that blowing dust out of the insides of PCs with cans of air was a great (albeit messy) idea, until an engineer pointed out that there was a good chance of actually forcing dust and dirt into the cracks and crevices of the electrical connectors inside the computer. Heck, some monitors require special cleaning solutions even to clean the dirt off the glass! I'm almost afraid to crack a cover anymore for fear of the damage outdoing the good.

Do It Right

Buy the highest quality computers you can, because cheap ones take more support and cause more problems than more expensive ones—not every time, but far too often to bet against it.

Duplicate It

Whatever you're buying, try to buy only one make and model and always set them up the same. Or, if you have to buy more than one type, try to minimize the differences as much as possible. Always set them up the same way. I've found a very effective way to do this is to create a working model, then copy the image of the entire hard disk up to the network. Whenever I need to install a new computer, I simply wipe out its local hard disk and copy down the master image from the network after booting up from a floppy. Afterward, I need to make only the personality changes (TCP/IP addresses, LU assignments, user or computer name, and so on). Whenever I want to make a change to my workstations, I use the master image from the network as a model, and figure out the best way to make the changes to it. Of course, this only works as long as users aren't customizing their individual configurations too much.

Document It

In my opinion, the toughest thing to do on a network is to document and track the configurations of the workstations. There are so many things to track that the effort is overwhelming. These are some of the things that you might have to take into account when planning to fix or upgrade a group of workstations: boot-up configuration (contents and specifics of CONFIG.SYS and AUTOEXEC.BAT), DOS version (and REV level), Windows version and whether all are local or not, ROM BIOS version, NIC BIOS level, whether the NIC has a BNC or UTP port or both, NIC type, available card slots, available drive bays, video card type, number of serial or parallel ports, other equipment installed (sound cards, SCSI adapters, and so on), mouse type (PS/2 port, bus card, or serial port), free disk space, serial number, user name, user location, and station jack ID. No matter how sophisticated and complete the inventorying software is, I seem to always have to go out and document something by hand. The more you can collect automatically and electronically, though, the better off you'll be. Don't expect any package to do it all for you. I recommend using the best workstation inventorying package you can afford, but understand that you'll probably have to document something the next time you consider making wholesale changes to your workstations.

Dos and Don'ts

Don't crack a case unless you really have to. Try to keep workstations out of harm's way and never lay them flat on the floor (the dirtiest and dustiest computers are those placed flat on the floor). I prefer putting all workstations on the floor in a vertical position with just the keyboard and monitor on the desktop. Make sure the workstation will not fall over or be smacked by a foot or an opening drawer.

AC Power

Put a good quality surge suppresser on each workstation, or use a UPS if you are in an area subject to frequent power fluctuations. Make sure that there are no laser printers,

Chapter 22—Network Preventive Maintenance

fans, coffee pots, heaters, or other non-workstation related devices plugged into the workstation's surge suppresser. Laser printers create severe voltage sags every time they reheat the fusing roller—this happens every 40 seconds or so, and is hard on the workstation's circuitry. Everything else mentioned is just “noisy” and is exactly what you are trying to protect the workstation from. Here's a rule of thumb: the computer, monitor, and anything required by the computer can be together, but no printers at all. The printer, even if it isn't a laser printer, should have its own surge suppresser just to be safe. Double-check that the power cord is firmly plugged into the back of each unit. The surge suppresser must plug directly into an AC outlet, not into the end of a 15-foot extension cord. If you have to run an extension cord, make sure it is as thick as, or thicker than, the cord on the surge suppresser—plug *only* the surge suppresser into it.

LAN Connection

Make sure that the station jack is securely fastened to the wall or partition. Loose “biscuit jacks” on the floor are unacceptable; they get kicked around and eventually will cause problems. The station cable must be the same category level as the main wiring. Never, under any circumstances, use silver-satin phone cord for a station cable. Double-check that the station cable is plugged firmly into the NIC. If the station cable shows any signs of wear (loose connectors or cuts in the shielding), replace it immediately. Using a frayed or defective station cable is an invitation for workstation failure.

Hardware

Use the best equipment you can talk the financial folks into buying, and purchase as few different models as possible. Purchase everything from one manufacturer if you can. (That way, you only have to create a relationship with one tech support department!) Standardize as much as you can, but realize that you'll never be able to standardize everything.

Operating Systems

Keep everyone running the same version and revision number of the operating system, even if it means removing newer versions from recently purchased computers. Better to face the devil you know than the one you don't. New versions might solve some bugs you've had to work around on the older version—but they are almost guaranteed to create new problems for which you will have to figure out solutions.

Try to keep everyone using the same version; upgrade only after complete and thorough testing of the new version. Being the first one on your block to load the newest version of any program simply means you get to be first to crash and burn. You can always spot the pioneers—they're the ones with all the arrows in their backs. Here's a rule of thumb: If a version number ends in .0, skip it. Wait for the .01 or the .1—nine times out of ten, the wait is well worth the lost headaches and aggravation.

Applications

Everything that is true for operating systems is true for application programs. To make life simpler, more maintainable, and much more reliable, I advocate loading all applications on the network only. It's much easier to support and upgrade one configuration on the network, rather than a separate configuration on each workstation across the

network. What might be lost in customizability and performance is certainly made up by reductions in support, maintenance costs, and downtime. Centralized applications should invalidate anyone's argument that the network is down too often to depend on.

Data

Users are notorious for expecting data they save on their local hard disks to be magically backed up by the network. While this functionality is available, it is neither common nor completely effortless to configure and implement. (And it never works if users turn off their computers at the end of the day!)

To prevent data loss, I try to set up all applications, whether loaded on the local drive or the network, to save by default to a user directory on the network. I let users know that this can be overridden if they want to save to a floppy or their local hard disk, but that by doing so they'll risk not having the data backed up in case of a drive problem.

Servers

I'm leery of cracking the case on a workstation, and therefore I'm practically terrified to crack the case on a file server. While dropping a screw or bending a connector on a workstation might inconvenience a user for a day or so while I get the PC repaired, the same simple error on the file server will inconvenience *me* until I get it back up and running. This is a reason to never make any changes to the file server an hour before everyone starts work. You'll end up starting your explanation of the prolonged server problem by saying, "All we had to do was..." or "It was supposed to be a five-minute job that..." Try working early on Saturday mornings instead. That gives you all day Saturday and Sunday to recover from a failure if one occurs. Other than that, the same admonitions and advice given for workstations also apply for servers.

Printers

Printers are arguably the most complex and maintenance-hungry components of a LAN. Just the fact that these devices can pick up only one piece of paper at a time, feed it through a series of rollers and guides without tearing it to shreds, and print something intelligible on it is amazing. Laser printers not only do that, but also bounce a beam of laser light off a rotating mirror, onto a drum that circulates through a cloud of carbon particles and creates text and graphics on a piece of paper. By definition, a laser printer actually prints using smoke and mirrors! Yet I find that most, if not all, printers are ignored and under-maintained. The only time they usually get any attention is when they finally fail.

Do It Right

Buy the best quality printers you can afford. Keep in mind that cheaper printers or off-brand printers can only claim to emulate the printer you know you ought to buy. "Emulate" means that an off-brand printer tries to work almost as well as the name-brand printer. I've discovered the hard way that the best way to find out what "almost" means

Chapter 22—Network Preventive Maintenance

is to have the president's assistant print out information for the president to present to a board meeting about fifteen minutes before the meeting starts. That's when you'll find out that it doesn't do landscape printing, the font spacing is erratic, the gray-shades don't work, or the graphs print only partway down the page.

Duplicate It

It's impossible, of course, to buy a new HP Series II printer these days to match your existing units. No one would be silly enough, I hope, to purchase an HP 4V and only use HP II drivers with it. So, what's a person to do? Just keep things as consistent as possible, and whenever you do install more than one of the same type of printer, configure them identically.

Document It

Never, under any circumstances, loan out the user's manual for a printer. Keep it in a safe if you have to. It is almost impossible to guess, remember, or figure out how to configure a printer. If your printer has lost its settings or someone has changed them, you'll need the manual in order to know how to reconfigure it. Knowing how to reconfigure the printer is only half the battle—if you haven't documented the working configuration, you'll have to start from scratch again. It's easy to waste half a day or more getting all the settings exactly right. Even then, invariably, someone will complain that their spreadsheets "just don't print the same anymore." In a pilfer-proof safe you should keep a user's manual and configuration listing for each printer. Woe to anyone who makes a change and doesn't document it! There's no feeling quite like having spent all morning to get a printer configured according to the latest documented configuration, then having users waltz in and say, "Yeah, now it's working like it was three months ago before Sally did something to make it work right. Please fix it that way again!"

Dos and Don'ts

How balanced is your printer sharing? Are all your printers being worked equally? Do you even have any idea how many pages each printer is printing per day/week/month? Is that old HP II still churning out all the end-of-month reports as well as the daily sales logs while the newer IIIsi idles along, producing an occasional memo or screen print? I once went to each of four laser printers and printed out the page count on Monday morning. After the fourth Monday I realized that one printer was printing over 50% of all pages printed for the company. By changing who printed to each printer, I was able to equalize the loading.

Remember that every printer has a recommended duty cycle (usually described as the maximum number of pages per month) and if your printers exceed this, you're more apt to have problems. If you have one printer doing more work than others, it makes sense to rotate them in and out of the "hot spot" so you don't have a premature failure. But to find potential problems like that, you have to know how much you are printing every month. If the configuration/monitoring software you install allows you to check a Pages Printed value, you can easily document this data. Otherwise, you need someone to do a test print and get it to you. A regular copy of the test print allows you to see if anyone is fooling with the printer's setup, too!

Keep it clean! Unlike PCs, printers really thrive and appreciate being cleaned out on a regular basis. Clean off the corona wires and get any excess paper gunk out of the feed assembly; always follow the manufacturer's recommendations.

Gateways and Routers

While it is easy to think of a LAN as just a server with some workstations and printers, it is rarely ever that simple. Most businesses require at least one connection to another system—a mainframe or mini, the Internet, or just another LAN. It is not uncommon to have a LAN connected to all three at the same time, which means that if the gateway or router device stops functioning, users are going to feel like the whole LAN is down. While most of us have had prior experience and knowledge of the server and workstations on a company's LAN, it is rare for individuals to have had formal training or education about gateways, routers, and other connective devices on any particular LAN. This situation is exacerbated by the fact that these devices are frequently installed and configured by “experts” with only cursory (if any) certification or training. Also, since these connective devices typically are plugged into something other than just another LAN, one needs to be somewhat conversant in the operations of the other system in order to really work with the device. In other words, if you don't know the difference between an LU and a CPU, you'll probably get pretty confused trying to reconfigure an SNA gateway that has just crashed.

It's not enough to have the mainframe staff tell you that the LU ID for a particular port needs to be changed from one value to another. If you don't know how to fire up the software to reconfigure the gateway, let alone how to run it, how can you possibly be expected to cope?

One time, when I was brought in to reconfigure a gateway, the controlling software required a password in order to change some simple, well-documented operating values. The gateway had been up and running for so long that the person who had last set the password was no longer with the company. What could have taken 15 minutes ended up taking several hours, since we had to completely reinstall the software with a new password. Fortunately, the system was still running and we could document all the configuration settings before we had to rebuild the gateway!

Do It Right

Realize that since the systems on each side of a connective device are changing all the time, it is unreasonable to expect one device to continue serving you perfectly over time. You usually will be notified of a need to change the gateway or router after you have made some minor change that renders the device inoperative. No matter how “right” your choice and installation of a gateway or router is the first time, the device is doing a tough job at a fundamental level of LAN operations. Pay these devices as much attention and treat them with as much respect as your file server, and you'll probably sprout gray hairs at a slower rate.

Duplicate It

By all means, use only one kind of device for each function. I use the same rule of thumb for gateways and routers that I use for hubs and MAUs: Try not to mix models, and don't ever mix vendors.

Document It

Just as with printers, you not only need to document the working configuration of gateways or routers, but have to keep documentation available that explains how to change the configuration. Trying to figure it out by loading various programs and searching Help files is a major waste of time and energy. Keep the user's manual, backup copies of programs, and a printout of the latest configuration parameters for each device in a safe place.

Dos and Don'ts

Don't take these devices for granted! They need care and feeding just as the file server does. Always follow the manufacturer's recommendations.

Summary

It's clear that a good NPM program requires much more than just following vendors' recommended cleaning and adjusting procedures. Unless your NPM program is built on a strong foundation of doing the job right the first time, duplicating systems and installations whenever possible, and documenting all configurations and procedures, it won't be effective. The three Ds can compensate for each other. If you can't get everything done exactly right, then by duplicating your work you can simplify debugging and upgrading. If you are unable to achieve duplication, then by documenting everything you do, you can understand the scope of what you're dealing with before you try to implement changes or repairs. Without documentation, you'll waste much effort during maintenance, upgrades, or disaster recovery.